

(51) International Patent Classification:  
**H04L 9/32** (2006.01)

TRAORE, Jacques [FR/FR]; 23 Avenue de la Suisse Normande, F-61100 SAINT GEORGES DES GROSEILLERS (FR).

(21) International Application Number:  
PCT/EP2005/002162

(74) Agents: JOLY, Jean-Jacques et al.; Cabinet Beau de Loménie, 158 Rue de l'Université, F-75340 PARIS Cedex 07 (FR).

(22) International Filing Date:  
28 February 2005 (28.02.2005)

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(25) Filing Language:  
English(26) Publication Language:  
English(30) Priority Data:  
04290557.0 2 March 2004 (02.03.2004) EP

(71) Applicant (for all designated States except US): FRANCE TELECOM [FR/FR]; 6 Place d'Alleray, F-75015 PARIS (FR).

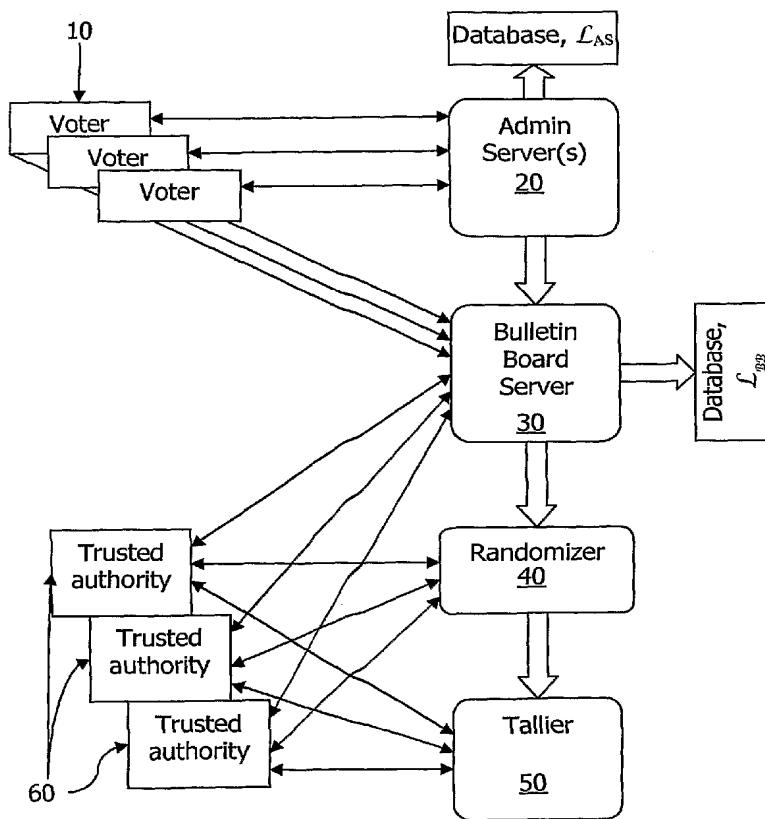
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

(72) Inventors; and

(75) Inventors/Applicants (for US only): CANARD, Sébastien [FR/FR]; 15 Rue Alexandre Bigot, F-14000 CAEN (FR). GAUD, Matthieu [FR/FR]; 18 Quai des Alliers, F-14470 COURSEULLES SUR MER (FR).

[Continued on next page]

(54) Title: ELECTRONIC VOTING PROCESS USING FAIR BLIND SIGNATURES



**(57) Abstract:** In an electronic voting process, a voter ( $V_i$ ) encrypts his vote ( $v_i$ ) according to the encryption scheme ( $E_v$ ) of a tallier mix-net (50) used to tally up the votes cast. The voter ( $V_i$ ) obtains on his encrypted vote, ( $x_i$ ), from an admin server module (20), a digital signature according to a fair blind signature scheme (FBSS). The encrypted vote ( $x_i$ ) is encrypted a second time, together with the unblinded digital signature ( $y_i$ ) thereof by the admin server, using the encryption scheme ( $E_M$ ) of a randomizing mix-net (40), to yield an output ( $c_i$ ), and the voter uses his own signature scheme ( $S_i$ ) to sign this, giving ( $\sigma_i$ ). The voter sends an ID code and data including ( $c_i, \sigma_i$ ) to a bulletin board server (30). Discrepancies in this vote data can be detected and their origin traced by prompting the randomizing mix-net servers (40) to provide proofs of correctness, and using the signature-tracing mechanism of FBSS.



European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**(88) Date of publication of the international search report:**  
26 May 2006

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*